(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2004 (15.04.2004)

PCT

(10) International Publication Number
WO 2004/032557 A1

(51) International Patent Classification[7]: H04Q 7/38, H04L 9/32

(21) International Application Number: PCT/SE2003/001461

(22) International Filing Date: 17 September 2003 (17.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/416,272 7 October 2002 (07.10.2002) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (publ)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NÄSLUND, Mats** [SE/SE]; Grimstagatan 161, S-162 58 Vällingby (SE). **NORRMAN, Karl** [SE/SE]; c/o Blomdahl, Tjustgatan 2, 5 tr., S-118 27 Stockholm (SE). **GOLDBECK-LÖWE, Tomas** [SE/SE]; Fleminggatan 40E, S-112 33 Stockholm (SE).

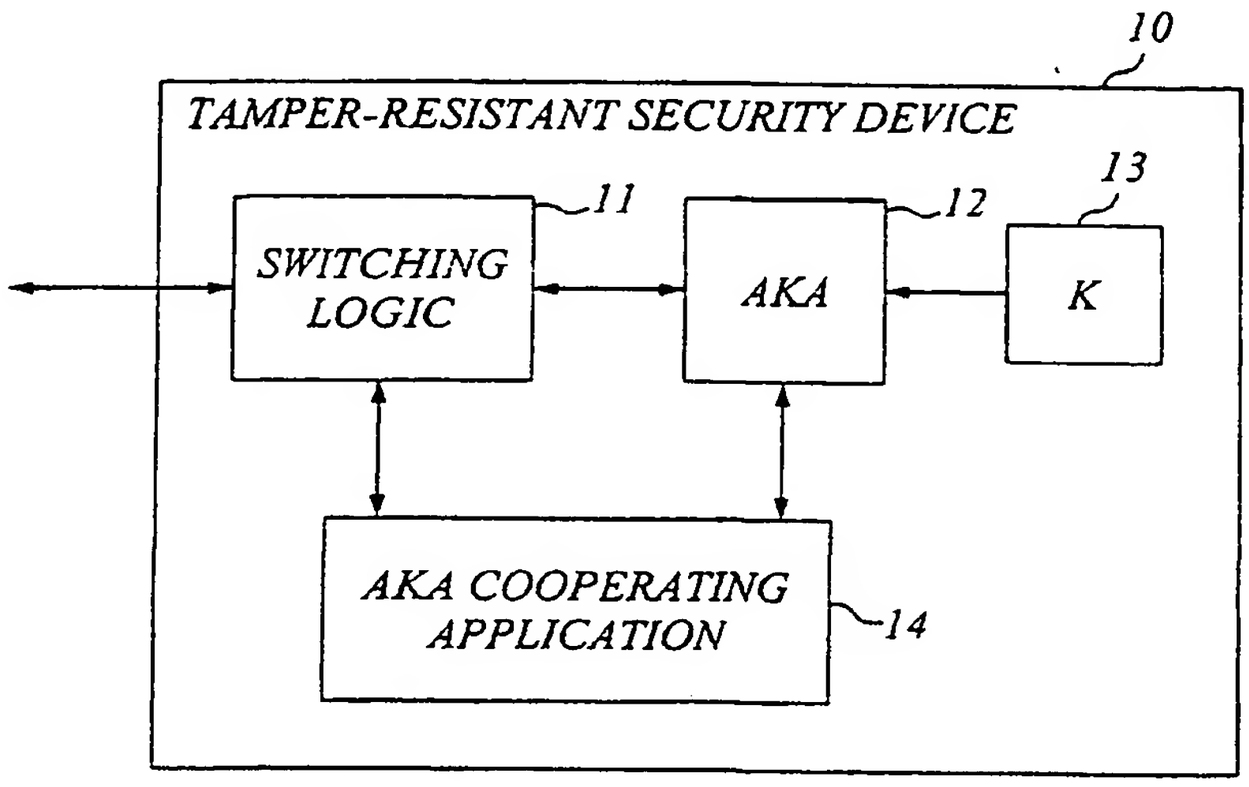
(74) Agent: **AROS PATENT AB**; P.O. Box 1544, S-751 45 Uppsala (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, EG, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK (utility model), SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,

*[Continued on next page]*

(54) Title: SECURITY AND PRIVACY ENHANCEMENTS FOR SECURITY DEVICES




(57) Abstract: The invention generally relates to a tamper-resistant security device, such as a subscriber identity module or equivalent, which has an AKA (Authentication and Key Agreement) module for performing an AKA process with a security key stored in the device, as well as means for external communication. The idea according to the invention is to provide the tamper-resistant security device with an application adapted for cooperating with the AKA module and means for interfacing the AKA module and the application. The application cooperating with the AKA module is preferably a security and/or privacy enhancing application. The application is advantageously a software application implemented in an application environment of the security device. For increased security, the security device may also be adapted to detect whether it is operated in its normal secure environment or a foreign less secure environment, and set access rights to resident files or commands that could expose the AKA process or corresponding parameters accordingly.

WO 2004/032557 A1

ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations. refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *with international search report*